WHAT IS CLAIMED IS:

1. A method for detecting network misconfigurations comprising:

identifying a remote target;

transmitting a forward packet series on a data path to the remote target;

receiving at least some packets from a reverse packet series transmitted on the data path from the remote target;

determining forward path performance characteristics for transmission of the forward packet series;

determining reverse path performance characteristics for transmission of the reverse packet series; and

if the forward path performance characteristics and the reverse path performance characteristics indicate asymmetry on the data path, generating an alert signaling a potential network misconfiguration of the data path.

2. The method of Claim 1, wherein the forward path performance characteristics indicate a forward packet loss rate for the forward packet series, and the reverse path performance characteristics indicate a reverse packet loss rate for the reverse packet series.

3. The method of Claim 1, wherein the forward path performance characteristics indicate a forward path throughtput on the data path, and the reverse path performance characteristics indicate a reverse path throughput on the data path.

4. The method of Claim 1, wherein the forward path performance characteristics and the reverse path performance characteristics each comprise a plurality of measurements each indicating performance of the data path for a particular time period.

5. The method of Claim 1, further comprising:

prior to transmitting the forward packet series, transmitting a pre-test packet to the remote target and receiving a pre-test acknowledgment from the remote target;

after transmitting the forward packet series, transmitting a post-test packet to the remote target and receiving a post-test acknowledgement from the remote target; and

determining the number of packets within the reverse packet series based upon a comparison of the pre-test acknowledgment and the post-test acknowledgment.

6. The method of Claim 5, wherein determining the number of packets within the reverse packet series comprises determining the difference between an internet protocol identifier within the post-test acknowledgment and an internet protocol identifier within the pre-test acknowledgment.

7. The method of Claim 1, wherein the remote target is configured to transmit the reverse packet series in response to a test request message, the method further comprising transmitting the test request message to the remote target prior to transmitting the forward packet series.

8. The method of Claim 1, further comprising establishing a transmission control protocol (TCP) communication session with the remote target prior to transmitting the forward packet series.

9. The method of Claim 8, wherein each packet within the forward packet series comprises a non-sequential TCP packet sequence number.

10. The method of Claim 1, wherein each packet within the forward packet series comprises an internet control message protocol (ICMP) echo/reply message.

11. The method of Claim 1, wherein the forward packet series comprises a plurality of packet bursts, each separated by a time constant.

12. The method of Claim 11, wherein each of the packet bursts comprises one or more packets separated by a second time constant.

13. The method of Claim 1, wherein each packet in the forward packet series has a size of 512 bits.

14. The method of Claim 13, wherein the forward packet series is communicated with protocol settings such that each packet in the reverse packet series has size of 512 bits.

15. The method of Claim 1, wherein the potential network misconfiguration signaled is an Ethernet duplexity mismatch.

16. The method of Claim 1, further comprising, if the forward path performance characteristics and the reverse path performance characteristics indicate asymmetry on the data path:

determining that the data path comprises a plurality of links;

identifying a second remote target on the data path;

transmitting a second forward packet series on the portion of the data path to the second remote target;

receiving at least some packets from a second reverse packet series transmitted on the portion of the data path from the second remote target;

determining second forward path performance characteristics for transmission of the second forward packet series;

determining second reverse path performance characteristics for transmission of the second reverse packet series; and

if the second forward path performance characteristics and the second reverse path performance characteristics indicate asymmetry on the portion of the data path, generating an alert signaling a potential network misconfiguration of the portion of the data path.

17. An analysis device comprising:

a network interface operable to couple to a remote target, to transmit a forward packet series on a data path to the remote target, and to receive at least some packets from a reverse packet series transmitted on the data path from the remote target; and

a controller operable to determine forward path performance characteristics for transmission of the forward packet series, to determine reverse path performance characteristics for transmission of the reverse packet series, and if the forward path performance characteristics and the reverse path performance characteristics indicate asymmetry on the data path, to generate an alert signaling a potential network misconfiguration of the data path.

18. The analysis device of Claim 17, wherein the forward path performance characteristics indicate a forward packet loss rate for the forward packet series, and the reverse path performance characteristics indicate a reverse packet loss rate for the reverse packet series.

19. The analysis device of Claim 17, wherein the forward path performance characteristics indicate a forward path throughtput on the data path, and the reverse path performance characteristics indicate a reverse path throughput on the data path.

20. The analysis device of Claim 17, wherein the forward path performance characteristics and the reverse path performance characteristics each comprise a plurality of measurements each indicating performance of the data path for a particular time period.

21. The analysis device of Claim 17, wherein:

the network interface is further operable, prior to transmitting the forward packet series, to transmit a pre-test packet to the remote target and to receive a pre-test acknowledgment from the remote target, and after transmitting the forward packet series, to transmit a post-test packet to the remote target and to receive a post-test acknowledgement from the remote target; and

the controller is further operable to determine the number of packets within the reverse packet series based upon a comparison of the pre-test acknowledgment and the post-test acknowledgment.

22. The analysis device of Claim 21, wherein the controller is further operable to determine the number of packets within the reverse packet series by determining the difference between an internet protocol identifier within the post-test acknowledgment and an internet protocol identifier within the pre-test acknowledgment.

23. The analysis device of Claim 17, wherein the remote target is configured to transmit the reverse packet series in response to a test request message, the network interface further operable to transmit the test request message to the remote target prior to transmitting the forward packet series.

24. The analysis device of Claim 17, wherein the network interface is further operable to establish a transmission control protocol (TCP) communication session with the remote target prior to transmitting the forward packet series.

25. The analysis device of Claim 24, wherein each packet within the forward packet series comprises a non-sequential TCP packet sequence number.

26. The analysis device of Claim 17, wherein each packet within the forward packet series comprises an internet control message protocol (ICMP) echo/reply message.

27. The analysis device of Claim 17, wherein the forward packet series comprises a plurality of packet bursts, each separated by a time constant.

28. The analysis device of Claim 17, wherein each of the packet bursts comprises one or more packets separated by a second time constant.

29. The analysis device of Claim 17, wherein each packet in the forward packet series has a size of 512 bits.

30. The analysis device of Claim 29, wherein the forward packet series is communicated with protocol settings such that each packet in the reverse packet series has size of 512 bits.

31. The analysis device of Claim 17, wherein the potential network misconfiguration signaled is an Ethernet duplexity mismatch.

32. The analysis device of Claim 17, wherein if the forward path performance characteristics and the reverse path performance characteristics indicate asymmetry on the data path, and if the data path comprises a plurality of links:

the network interface further operable to transmit a second forward packet series on the portion of the data path to the second remote target, and to receive at least some packets from a second reverse packet series transmitted on the portion of the data path from the second remote target; and

a controller operable to determine second forward path performance characteristics for transmission of the second forward packet series, to determine second reverse path performance characteristics for transmission of the second reverse packet series, and if the second forward path performance characteristics and the second reverse path performance characteristics indicate asymmetry on the portion of the data path, to generate an alert signaling a potential network misconfiguration of the portion of the data path.

33. Logic for detecting network misconfigurations, the logic encoded in media and operable when executed to perform the steps of:

identifying a remote target;

transmitting a forward packet series on a data path to the remote target;

receiving at least some packets from a reverse packet series transmitted on the data path from the remote target;

determining forward path performance characteristics for transmission of the forward packet series;

determining reverse path performance characteristics for transmission of the reverse packet series; and

if the forward path performance characteristics and the reverse path performance characteristics indicate asymmetry on the data path, generating an alert signaling a potential network misconfiguration of the data path.

34. The logic of Claim 33, wherein the forward path performance characteristics indicate a forward packet loss rate for the forward packet series, and the reverse path performance characteristics indicate a reverse packet loss rate for the reverse packet series.

35. The logic of Claim 33, wherein the forward path performance characteristics indicate a forward path throughtput on the data path, and the reverse path performance characteristics indicate a reverse path throughput on the data path.

36. The logic of Claim 33, wherein the forward path performance characteristics and the reverse path performance characteristics each comprise a plurality of measurements each indicating performance of the data path for a particular time period.

37. The logic of Claim 33, further operable when executed to perform the steps of:

prior to transmitting the forward packet series, transmitting a pre-test packet to the remote target and receiving a pre-test acknowledgment from the remote target;

after transmitting the forward packet series, transmitting a post-test packet to the remote target and receiving a post-test acknowledgement from the remote target; and

determining the number of packets within the reverse packet series based upon a comparison of the pre-test acknowledgment and the post-test acknowledgment.

38. The logic of Claim 37, wherein determining the number of packets within the reverse packet series comprises determining the difference between an internet protocol identifier within the post-test acknowledgment and an internet protocol identifier within the pre-test acknowledgment.

39. The logic of Claim 37, wherein the remote target is configured to transmit the reverse packet series in response to a test request message, the logic further operable when executed to perform the step of transmitting the test request message to the remote target prior to transmitting the forward packet series.

40. The logic of Claim 33, further operable when executed to perform the step of establishing a transmission control protocol (TCP) communication session with the remote target prior to transmitting the forward packet series.

41. The logic of Claim 40, wherein each packet within the forward packet series comprises a non-sequential TCP packet sequence number.

42. The logic of Claim 33, wherein each packet within the forward packet series comprises an internet control message protocol (ICMP) echo/reply message.

43. The logic of Claim 33, further operable, if the forward path performance characteristics and the reverse path performance characteristics indicate asymmetry on the data path, to perform the steps of:

determining that the data path comprises a plurality of links;

identifying a second remote target on the data path;

transmitting a second forward packet series on the portion of the data path to the second remote target;

receiving at least some packets from a second reverse packet series transmitted on the portion of the data path from the second remote target;

determining second forward path performance characteristics for transmission of the second forward packet series;

determining second reverse path performance characteristics for transmission of the second reverse packet series; and

if the second forward path performance characteristics and the second reverse path performance characteristics indicate asymmetry on the portion of the data path, generating an alert signaling a potential network misconfiguration of the portion of the data path.

44. An analysis device comprising:

means for identifying a remote target;

means for transmitting a forward packet series on a data path to the remote target;

means for receiving at least some packets from a reverse packet series transmitted on the data path from the remote target;

means for determining a forward packet loss rate for the forward packet series;

means for determining a reverse packet loss rate for the reverse packet series; and

means for, if the forward packet loss rate and the reverse packet loss rate differ by at least a threshold amount, generating an alert signaling a potential network misconfiguration of the data path.